CLAIMS

1. A method of recording transmitted digital data in which transmitted digital information is encrypted by a recording encryption key (E(NE)) and stored by a recording means ~~(50)~~ on a recording support medium and characterised in that an equivalent of the recording encryption key (E(NE)) is encrypted by a recording transport key (RT(A)) and stored on the support medium together with the encrypted information.

2. A method as claimed in claim 1 in which the information encrypted by the recording encryption key (E(NE)) comprises control word information (CW) usable to descramble a scrambled data transmission also recorded on the support medium.

3. A method as claimed in claim 1 ~~or 2~~ in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) are stored on a portable security module ~~(52)~~ associated with the recording means ~~(50)~~.

4. A method as claimed in ~~any preceding claim~~ claim 1 in which the transmitted information is encrypted prior to transmission and received by a decoder means ~~(12)~~ before being communicated to the recording means ~~(50)~~.

5. A method as claimed in claim 4 in which the decoder ~~(50)~~ is associated with a portable security module ~~(30)~~ used to store transmission access control keys (K0(NS), K0'(Op1,NS) etc.) used to decrypt the transmitted encrypted information.

6. A method as claimed in claim 5 in which the recording encryption key (E(NE)) and/or recording transport key (RT(A)) function in accordance with a first encryption algorithm (DES) and the transmission access control keys (K0(NS), K0'(Op1,NS) etc.) function in accordance with a second encryption algorithm (CA).

7. A method as claimed in ~~any preceding claim~~ claim 1 in which the recording transport key (RT(A)) is generated at a central recording authorisation unit ~~(21,24,25)~~ and a copy

of this key communicated to the recording means ~~(50)~~.

8. A method as claimed in claim 7 in which the recording transport key (RT(A)) is preferably encrypted by a further encryption key (K0(NSIM)) prior to being communicated to the recording means ~~(50)~~.

9. A method as claimed in ~~any preceding claim~~ claim 1 in which a central access control system ~~(21,24,25)~~ communicates transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to the recording means ~~(50)~~.

10. A method as claimed in claim 9 in which the transmission access control keys (K0(NS), K0'(Op1,NS) etc.) are communicated to a portable security module ~~(52)~~ associated with the recording means ~~(50)~~.

11. A method as claimed in claim 9 ~~or 10~~ in which the recording means ~~(50)~~ directly descrambles transmitted information using the transmission access keys (K0(NS), K0'(Op1,NS) etc.) prior to re-encryption of the information by the recording encryption key (E(NE)) and storage on the support medium.

12. A method as claimed in ~~any of claims 9, 10 or 11~~ claim 9 in which the central access control system ~~(21, 24, 25)~~ preferably encrypts the broadcast access control keys (K0(NS), K0'(Op1,NS) etc.) by a further encryption key (K0(NSIM)) prior to their communication to the recording means ~~(50)~~.

13. A method as claimed in ~~any of claims 9 to 12~~ claim 9 in which the recording means ~~(50)~~ sends a request to the central access control system including information identifying the broadcast access keys needed (K0(NS), K0'(Op1,NS) etc.), the request being authentified by the recording means ~~(50)~~ using a key (K0(NSIM)) unique to that recording means.

14. A method as claimed in claim 1 using a decoder means ~~(12)~~ and associated security module ~~(30)~~ and a recording means ~~(50)~~ and associated security module ~~(52)~~

and in which a copy of the recording transport key (RT(A)) is stored in the security module ~~(30)~~ associated with the decoder means ~~(12)~~ and/or the security module ~~(52)~~ associated with the recording means.

15. A method as claimed in claim 14 in which the recording transport key (RT(A)) is generated by either the recording security module ~~(52)~~ or decoder security module ~~(30)~~ and communicated to the other security module.

16. A method as claimed in claim 15 in which the recording transport key (RT(A)) is preferably encrypted before communication to the other security module and decrypted by a key unique (K0(NS)) to that other security module.

17. A method as claimed in claim 16 in which the decoder security module ~~(30)~~ and recording security module (52) carry out a mutual authorisation process, the unique decryption key (K0(NS)) being passed to the other security module from the encrypting security module depending on the results of the mutual authorisation.

18. A method as claimed in claim 17 in which the mutual authorisation step is carried out using, inter alia, an audience key K1(C) known to both security modules (30,52).

19. A method as claimed in ~~any of claims 14 to 18~~ claim 14 in which the decoder security module ~~(30)~~ possesses transmission access control keys (K0(NS), K0'(Op1,NS) etc.) to decrypt the transmitted information in an encrypted form and a session key (K3(NSIM)) re-encrypt the information prior to communication to the recording security module ~~(52)~~, the recording security module ~~(52)~~ possessing an equivalent of the session key (K3(NSIM)) to decrypt the information prior to encryption by the recording transport key (RT(A)).

20. A method as claimed in claim 19 in which the session key (K3(NSIM)) is generated by the decoder security module or recording means security module ~~(52)~~ and communicated to the other module in encrypted form using an encryption key

(K0(NS)) uniquely decryptable by the other security module.

21. A recording means ~~(50)~~ adapted for use in a method as claimed in ~~any preceding claim~~ claim 1 comprising a security module ~~(52)~~ for encrypting transmitted digital information by a recording encryption key (E(NE)) for storage on a recording support medium and characterised in that the security module ~~(52)~~ is further adapted to encrypt the recording encryption key (E(NE)) by a recording transport key (RT(A)) for storage on the support medium.

22. A portable security module ~~(52)~~ adapted for use in the recording means of claim 21 and characterised in comprising a recording encryption key (E(NE)) for encryption of transmitted digital information for subsequent recordal and a recording transport key (RT(A)) for encryption of the recording encryption key for subsequent recordal.

23. A decoder means ~~(20)~~ adapted for use in a method as claimed in ~~any of claims 14 to 20~~ claim 14 including a security module ~~(30)~~ adapted to store a copy of the recording transport key (RT(A)).

24. A decoder means ~~(20)~~ as claimed in claim 23 including a security module ~~(30)~~ adapted to descramble transmitted information using one or more transmission access keys (K0(NS), K0'(Op,NS) etc.) prior to reencryption by a session key (K3(NSIM)) for subsequent communication to a recording means.

25. A portable security module ~~(30)~~ adapted for use in the decoder means ~~(20)~~ of claim 23 ~~or 24~~ and comprising at least a copy of the recording transport key (RT(A)).

~~26.~~ A method of recording transmitted digital data substantially as herein described.

27. A recording means substantially as herein described.

28. A portable security module substantially as herein described.

29. A decoder ~~means substantially~~ as herein described.